ARMY RESEARCH LABORATORY

Protecting and Securing a Web Portal of Presidential Electronic Records Archives

by Binh Nguyen, Son Nguyen, and Glenn Racine

ARL-TR-3338 September 2004

NOTICES

Disclaimers

Army Research Laboratory
Adelphi, MD 20783-1197

ARL-TR-3338 **September 2004**

Protecting and Securing a Web Portal of Presidential Electronic Records Archives

Binh Nguyen, Son Nguyen, and Glenn Racine
Computational and Information Sciences Directorate, ARL

REPORT DOCUMENTATION PAGE			*Form Approved* *OMB No. 0704-0188*

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED (From - To)**
September 2004	Final	April 2003 - June 2004

4. TITLE AND SUBTITLE	**5a. CONTRACT NUMBER**
Protecting and Securing a Web Portal of Presidential Electronic Records Archives	
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	**5d. PROJECT NUMBER**
Binh Nguyen, Son Nguyen, and Glenn Racine	
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	**8. PERFORMING ORGANIZATION REPORT NUMBER**
U.S. Army Research Laboratory ATTN: AMSRD-ARL-CI-CN 2800 Powder Mill Road Adelphi, MD 20783-1197	ARL-TR-3338
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	**10. SPONSOR/MONITOR'S ACRONYM(S)**
U.S. Army Research Laboratory 2800 Powder Mill Road Adelphi, MD 20783-1197	**11. SPONSOR/MONITOR'S REPORT NUMBER(S)**

12. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for public release; distribution unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

This document reports the findings of a 14-month study focused on the information-assurance (IA) tasks to enable the establishment of a secured Web portal of sensitive presidential records that will be operating in a public internetworking environment, the Internet II. This work is part of the ARL cooperative agreement number DAAD19-03-2-0018, an enabling vehicle for a joint science-and-engineering research project of ARL and Georgia Tech Research Institute (GTRI). The purpose of this collaborative work is to facilitate the processing and the protection of distributed authentic electronic records archives (ERA) for the U.S. National Archives and Records Administration (NARA). This IA research effort investigated security architecture, government-certified commercial IA products, and deployment issues.

15. SUBJECT TERMS

Information assurance, electronic records archives, web portal

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**	UL	42	Binh Nguyen
Unclassified	Unclassified	Unclassified			**19b. TELEPHONE NUMBER** *(Include area code)* (301) 394-1781

Standard Form 298 (Rev. 8/98)
Prescribed by ANSI Std. Z39.18

Preface

The U.S. Army Research Laboratory (ARL) prepared this technical report for submission to the U.S. National Archives and Records Administration (NARA). ARL conducts basic and applied research to provide the technological competitive edge for the U.S. Army. NARA is the record-keeper of the Nation; it is the steward of irreplaceable electronic and non-electronic collections documenting our Nation's experience, the actions of government, and the rights and entitlements of our citizens.

This document reports the findings of a 14-month study focused on the information-assurance (IA) tasks to enable the establishment of a secured Web portal of sensitive presidential records that will be operating in a public internetworking environment, the Internet II. This work is part of the ARL cooperative agreement number DAAD19-03-2-0018, an enabling vehicle for a joint science-and-engineering research project of ARL and Georgia Tech Research Institute (GTRI). The purpose of this collaborative work is to facilitate the processing and the protection of distributed authentic electronic records archives (ERA) for NARA. This IA research effort investigated security architecture, government-certified commercial IA products, and deployment issues.

INTENTIONALLY LEFT BLANK.

Contents

List of Figures

List of Tables

INTENTIONALLY LEFT BLANK.

Executive Summary

This document reports the findings of a study focused on the information-assurance (IA) tasks supporting the establishment of a secured Web portal of presidential electronic records under the Presidential Electronic Records Pilot Operating System (PERPOS) project. The task to set up the portal is a collaborative work between the U.S. Army Research Laboratory (ARL) and the Georgia Tech Research Institute (GTRI). GTRI tackles the functional aspects of the portal, and ARL undertakes part of the security aspects of the portal. The planned IA tasks included five technical tasks: (1) information assurance architectural framework for the experimental portal of sensitive electronic records, (2) commercial IA product assessment, (3) tools and techniques for the performance evaluation of the portal operating in secured and unsecured modes, (4) defensive IA product assessment and deployment, and (5) implementation and deployment issues. ARL completed three tasks (1, 3, and 4), canceled two tasks (2 and 5), and redistributed technical and financial resources for the continued research in the next phase of the project. ARL canceled two tasks because it needed to meet exigencies and ongoing operations associated with Operation Iraqi Freedom (OIF).

The accomplishments of the three tasks generated crucial findings necessary for and vital to the building of the portal at GTRI. They include (1) an IA architectural framework for securing and protecting the PERPOS portal, (2) methods, techniques, and software tools to determine the quantitative performance cost associated with the deployment of security products in the portal, (3) an evaluation and a recommendation for selecting a government-validated firewall suitable for the protection of the portal. The main themes of the IA architectural framework incorporate the use of government-validated defensive IA products, secure electronic commerce technology and services, and the defense-in-depth strategy. Successful quantitative performance measurement tools and techniques were prototyped and experimented in a virtual network of virtual machines to comparatively measure the performance of a web server operating in secured mode and unsecured mode. The same tools and techniques will be improved in the next phase of the project and used for measuring the performance of the actual physical Web portal at GTRI. The recommendation for selecting a firewall, including the results of an evaluation of 30 firewall products, is being acted on by the GTRI team to acquire and deploy an appropriate firewall to protect the PERPOS portal.

Initial results generated during the performance period provided encouraging evidence that form the basis for the coming efforts; therefore, ARL recommends that the following tasks be conducted in FY05:

Conduct empirical experiments to evaluate the performance overhead induced by the deployment of defensive IA products at the actual PERPOS portal operating in unsecured and secured mode.

The overhead will be measured in terms of elapsed times *and* computing times taken at the client computer.

Continue assessing intrusion detection systems, antiviral software, and security management tools suitable for the protection and the empirical experimentation of the actual PERPOS web server and develop a set of research performance metrics potentially applicable to measuring the efficacy of the IA products deployed to protect and secure the physical PERPOS portal.

1 Introduction

1.1 Background

Being the record-keeper of the Nation, the U.S. National Archives and Records Administration (NARA) conducts and sponsors research efforts to find innovative solutions for the persistent and authentic preservation of government electronic records archives (ERA). To provide geographically dispersed researchers and administrators with a convenient and secured means for accessing data and sharing research results over the Internet, NARA sponsors the setup of an experimental portal capable of protecting, storing, and delivering sensitive presidential ERA at the Georgia Tech Research Institute (GTRI), Atlanta, Georgia. The task to set up the portal is a collaborative work between the U.S. Army Research Laboratory (ARL) and GTRI. GTRI tackles the functional aspects of the portal, and ARL undertakes part of the security aspects of the portal.

1.2 Scope

This document reports the preliminary results of ARL-conducted research tasks that were directly and indirectly related to the distributed processing of ERA and the protection of the portal. The intended audience of this report includes ARL and NARA administrators and managers, ERA and information assurance (IA) researchers, and information technology personnel. The main purposes of this document are as follows:

- Reporting work accomplished during the reporting period
- Reporting changes to planned activities
- Recommending continued research activities for the next phase of the project.

The next section describes specific planned tasks, reports the status of each task and explains the method by which each task was accomplished and the reason(s) for which a task was changed or canceled. Section 3 presents and discusses the results of each accomplished task. Section 4 summarizes professional activities, including technical conference attendance, publication and presentation, training, and travels. Section 5 concludes the paper and recommends research activities to be accomplished during the next phase.

2. Project Status

The planned IA tasks for ARL to undertake include five technical tasks and a program management task, requiring an estimated level of effort of about 1.4 full-time equivalent (FTE) years and .2 FTE, respectively. Minor changes to the approach slightly affecting the scope of the project include the reassignment of planned expenditure of human and financial resources, resulting in the cancellation of two technical tasks. Completed tasks generated publishable research findings, which were presented in technical conferences. Table 1 delineates and summarizes the description of each task, its estimated and actual level of effort in term of full-time equivalent (FTE) years, and its status as of the end of the performance period. Subsequent paragraphs within this section explain the contents of the table. Section 3 reports and discusses the results of the accomplished tasks.

Table 1. Summary of tasks.

Task	Title	Planned FTE	Actual FTE	Status
1	Information Assurance Architecture	.1	.2	Completed
2	Commercial Product Assessment	.1	-	Canceled
3	Performance Evaluation	.4	.4	Completed
4	Technology Assessment and Deployment	.1	.3	Completed
5	Implementation and Deployment Issues	.7	-	Canceled
6	Program Management	.2	.2	Completed
	Total:	1.6	1.1	

3. Results and Discussions of Completed Tasks

This section provides an overview of the completed tasks together with any work that deviated from the original plans. Excluding the program management task, three out of six planned tasks were successfully completed. The accomplishments consist of (i) the development of an information assurance architectural framework for the experimental Web portal of sensitive ERA (Task 1), (ii) the building of a low-cost computing infrastructure for supporting the development of tools and techniques for the performance evaluation of the portal operating in secured and unsecured modes (Task 3), (iii) the selection of an appropriate firewall that will be used to safeguard the Web portal and a survey of suitable firewall products that have been evaluated and validated against the Common Criteria Evaluation and Validation Scheme and the Common Criteria Recognition Arrangement (Task 4), and (iv) the technical and managerial collaboration between internal departments, external research institutions, and all aspects of program management (Task 6).

3.1 Task 1: Information Assurance Architecture

3.1.1 Status

This task was completed with a recommended security architectural framework for the Presidential Electronic Records Pilot Operating System (PERPOS) portal that is being built by the GTRI as a convenient and low-cost means for sharing sensitive electronic presidential records and archival processing software tools. The portal will also provide indispensable IA services for the electronic archival records to provide their stakeholders with a reasonable assurance that the contents, structure, and context of the records are authentically preserved. The main themes of the recommended architecture incorporate the use of government-validated defensive IA products, secure electronic commerce technology and services, and the defense-in-depth strategy. The design was documented in the form of a technical conference paper, a copy of which was handed over to the GTRI team for references. Work on this task consumed more time than the principal investigator had originally planned. The actual time taken for this task was at least .2 FTE to complete a literature search of relevant technical papers, a design and analysis of an architectural framework, documenting, interpreting, publishing, and presenting the results at a technical security conference.

3.1.2 Results and Discussions

Web portals are ever-present in the World Wide Web, but an operational portal containing sensitive electronic records has not existed due to security concerns. Connecting a portal of such sensitive archival records to the Internet requires prudent care to reasonably assure the confidentiality and integrity of the records and to provide authentication, availability, and non-repudiation services for their stakeholders. The reason is simply that the Internet is a public network to which every Internet user is physically connected to the portal and that the threats to the portal and its electronic archival records are "real and present." A successful attack against the electronic archival records would potentially damage the reputation of their stakeholders, complicate the operation of the responsible organizations, and deprive future references to historical events.

The building of a Web portal of sensitive archives requires serious consideration of defensive security measures. Among the very first measures is the development of a security architectural framework for the building of an experimental portal. This portal will provide NARA administrators and its geographically dispersed researchers with convenient means for uploading and downloading sensitive presidential electronic records and processing tools, monitoring and sharing research results, and simultaneously performing empirical experiments with defensive security strategies, tactics, and technologies potentially capable of meeting the security requirements of a fully operational portal in the near future. The recommended architectural framework described in this report applies the technical facet of the defense-in-depth strategy (*2*) developed and widely implemented by the Department of Defense.

The defense-in-depth strategy requires the building of multi-layered defenses. The layers consist of (i) the network and infrastructure, (ii) the enclave boundary, (iii) the computing environment, and (iv) the supporting infrastructure. Although the strategy relies on people, operation, and technology, this task focused on the technology feature of the strategy by presenting an architectural framework and describing some proactive measures for safeguarding the experimental PERPOS portal containing sensitive electronic records.

Applying the defense-in-depth strategy, the networked computing environment in which the experimental PERPOS portal runs should be placed within an internal subnet of the information infrastructure of GTRI as illustrated in figure 1. The security measures of GTRI are presumed to provide some protection for the portal environment; however, further proactive approaches to safeguarding the portal and its contents still need to be implemented for added layers of defenses (Figure 2) to counter all types of attacks against the portal. The potential attacks consist of active, passive, inside, close in, and distribution types (*2*). The layered approach protects the network and infrastructure, the boundaries of the portal enclave, the computing environment, and the supporting infrastructure of the Web portal.

As shown in figure 1, the portal computing environment is inside the PERPOS research enclave but isolated from other computing systems within the research enclave. The portal environment directly connects to the Internet and has different security policies than other computing systems that are outside the portal environment. If the portal is compromised by a successful attack, it is prevented to be used by the attacker as a stepping stone for launching attacks against other systems within the research enclave and the information infrastructure of the Georgia Institute of Technology (Gatech).

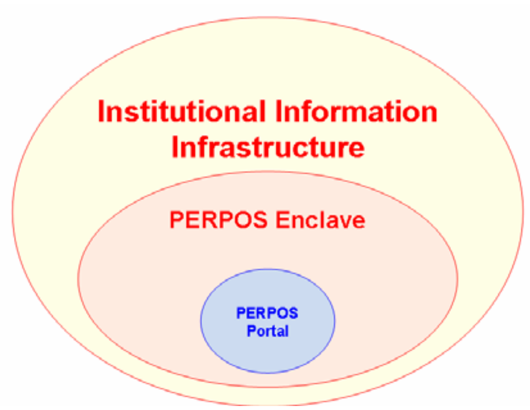


Figure 1. Portal environment.

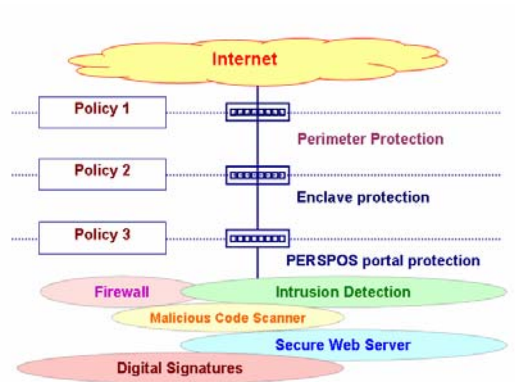


Figure 2. Layers of defense.

Safeguarding the portal computing environment includes implementation of technologies that can successfully secure and protect all five basic IA services offered by the portal. These five services are confidentiality, integrity, authentication, non-repudiation, and availability services. Confidentiality services provide a reasonable assurance that the contents of the archives are only disclosed to authorized users, while the archives are stored in the portal and the user's computer, and when they are uploaded to and downloaded from the portal. Integrity services ensure the wholeness of the ERA and provide a way for detecting a change to the archives. Authentication services provide mutual assurance of identities: the identity of the portal itself and the identity of its users. Non-repudiation services provide the stakeholders of the portal a way for obtaining credible evidence of the use of electronic archival records stored at the portal. Availability services ensure that the portal services are readily accessible to authorized users whenever the electronic archives are needed.

Incoming and outgoing packets traveling between the Internet and the portal must pass through several layers of defense. Each layer has its own set of security policy and defensive security measures. Although describing detailed defense mechanisms of the outer layers of the portal environments is outside the scope of this report, their functionality can be summarized as follows. The outermost layer usually has an overarching security policy that affects all users and the computing systems that are connected to the information infrastructure of the organization. The security policy applied at the enclave (e.g., electronic records research enclave) further limits access to research data, tools, and documents. The portal itself also has a security policy for accessing the portal and its sensitive electronic archives. Figure 2 illustrates this multi-layered defense mechanism.

Using an appropriate security policy at the very first line of defense, the outermost checkpoint inspects every incoming packet and decides whether the inspected packet should be dropped or sent to a destined subnet within the organizational infrastructure. Once an incoming packet has passed this inspection, it is subject to another similar inspection at the perimeter of the research enclave. If it passes the inspection, it is then routed to an appropriate destination within the research enclave. If the destination is the portal of electronic records, then the gatekeeper of the research enclave once again scrutinizes the incoming packet before sending it to the portal for services using the local security policy of the portal.

The security posture at the portal includes the employment of several defensive mechanisms for the protection of sensitive electronic archives and the physical assets deployed at the portal. All electronic accesses to the portal are considered to originate from untrusted networks; therefore, they must first go through the firewall and the intrusion detection system deployed at the portal computing enclave. The firewall inspects the header of each incoming packet and decides the fate of the packet. The intrusion detection system inspects the contents of incoming packets for possible malicious payload. These defensive mechanisms are also a way to prevent unauthorized insiders from accessing the portal. Figure 3 shows the security process at the portal environment.

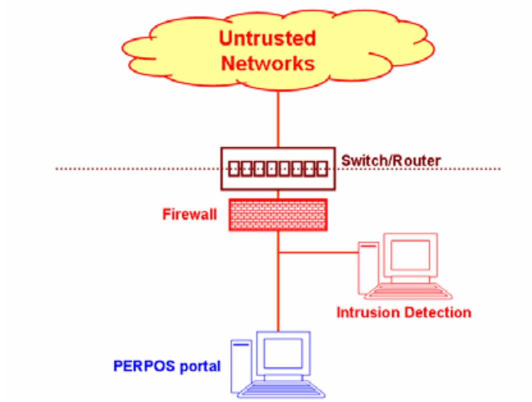


Figure 3. Security posture at the portal

Controlling access to the portal services consists of user authentication and authorization. The user authentication process verifies the identity of the user, which consists of the verification of the legitimacy and correctness of user-presented credentials, including digital certificates in combination of user name, password, or biometric information, and possibly the unique address of the computer from which the incoming packets originated. Once the user authentication is successful, the portal next sends its digital certificate to the user to provide the user with a reasonable assurance that the portal is the bona fide server of the sensitive electronic records. The digital certificates used by the user and the portal can be issued by the owner, the administrator of the electronic records, the administrator of the portal, or a third party that is mutually trusted by all the stakeholders of the sensitive electronic records. Authorization mainly concerns restricting the privileges of an authenticated authorized user to access a certain computing resource available at the portal. Authorization depends on the local security policy at the portal.

Monitoring access to the portal services includes logging all the activities that occur in the portal such that the logs can be used for creating credible proof of an activity performed by a user (non-repudiation). A provable activity could be sending a request for a particular electronic record or receiving a requested record. Protecting the integrity and availability of the portal consists of several proactive measures. Some of these preventive measures include:

- Avoiding potential distribution attacks (e.g., spy ware and Trojan horse) by deploying validated software and hardware products in the portal (*3*)
- Excluding unauthorized executable contents from being installed at the portal and scanning every newly stored electronic file for possible malicious code (e.g, viruses and worms)
- Rejecting incoming requests for unauthorized network services and monitoring potential abuses of authorized services (e.g., denial-of-service attacks)

- Detecting and preventing unauthorized changes to electronic records and system configuration by implementing access control mechanisms and by monitoring changes to system and data files as well as their attributes (e.g,. ownership, type, and permission)
- Preventing temporary loss of electrical power that the portal needs by connecting the portal to an uninterruptible power system having sufficient power to keep the portal up and running, while the main source of energy is being restored
- Backing up portal resources regularly for the replacement of lost or damaged electronic records and restoring system services
- Preventing close-in attacks by restricting access to the physical area of the portal, the computing and network infrastructure, and the source of electrical energy.

Validated countermeasure security products refer to commercially available software and hardware products whose claimed capabilities have been successfully evaluated against the Common Criteria for Information Technology Security Evaluation, which is also known as the Common Criteria (*3*). The acquisition and deployment of validated products provide a realistic assurance of acceptable protection of irreplaceable ERA.

Accessing the portal using a web browser (e.g., Microsoft Internet Explorer) is envisioned to be the primary means for accessing sensitive electronic archives as it is commonly used to conduct electronic commerce over the Internet. To buy a product over the Web, a potential customer is not usually required to have a digital certificate, but a legitimate vendor often relies on a digital certificate issued by a third party (e.g., Verisign) to gain the trust from a potential buyer. A communication scenario at the experimental portal differs from a commercial web site in that mutual authentication is required. A user of the portal must present a digital certificate to the portal for verification and validation of the presented identity. Commercially available cryptographic products and services that are enabling this type of secure electronic commerce activities (*4*) can meet some of the requirements for mutual authentication and for other IA services, including integrity, confidentiality, and non-repudiation services.

Given the current (128-bit) cipher strength of a typical web browser operating in a secure mode, the portal possesses only electronic records having a relatively low level of sensitivity. Using Type 1 cryptographic products to protect classified and highly sensitive electronic records stored at the portal is a possibility, but doing so will require additional expenses in terms of product acquisition costs and procedural and administrative overhead. Therefore, within the scope of this project, supporting geographically dispersed researchers and administrators, the use of commercial cryptographic products is sufficient. These IA services must be provided to protect sensitive electronic records in all information states. According to Maconachy, et al. (*5*), information is found in one or more of the three states: stored, processed, or transmitted.

3.1.3 Conclusions

The proposed security implementation at the portal can provide reasonable IA services for the electronic archival records just while they are stored at the portal and in transit. Once an electronic archival record has been transferred from the portal to an external host, it also needs IA services at the remote host to preserve its contents, structure, and context, especially while it is being processed.

3.2 Task 3: Performance Evaluation

3.2.1 Status

This task was to evaluate the performance of the secured portal operating in unsecured and secured mode by conducting experiments to observe and to measure the overhead associated with deployed cryptographic products. Instead of waiting for the construction of the experimental portal to be completed at the campus of GTRI under the PERPOS project, extra efforts were spent to build a low-cost computing infrastructure capable of providing a networked environment in which empirical experiments could be conducted to gather and analyze interim performance data.

The infrastructure environments also provided the principal investigator (PI) with necessary computing platforms to successfully develop methods, techniques, and automated software tools capable of systematically automating the extraction of appropriate performance data and formatting the results. The prototypes of these tools were used in the test bed to experiment with an emulated portal running in various configurations. The results and findings are reported below and also documented for possible submission to technical conferences for peer review and acceptance for possible presentation and publication.

3.2.2 Results and Discussions

Two low-cost networked systems have been constructed on a notebook computer to support an interim experimentation process, a short-term process while the actual PERPOS portal is being established at the campus of GTRI. The first system is a virtual environment consisting of a network of virtual machines running the Linux (http://www.linux.org) operating systems (OS) (figure 4). The second system is a physical environment running the Microsoft Windows XP (http://www.microsoft.com/windowsxp) having different applications (figure 5).

Within the virtual network environment, a virtual machine runs the open-source *Apache* web server (http://www.apache.org) capable of operating in secured and unsecured modes, and the other virtual machines run a web client (figure 4). The Linux OS running in the virtual environment offers interactive and non-interactive downloading files from the Apache web server using the *Mozilla* web browser (http://www.mozilla.org) and the *wget* command, respectively. Network connections among the virtual machines are accomplished through the use of a virtual switch.

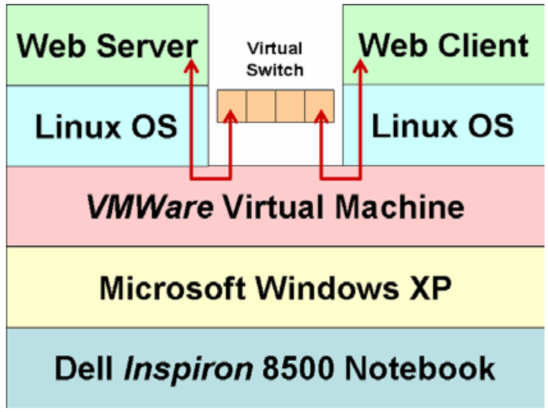


Figure 4. Virtual Network Environment (VNE).

The other experimental networked system is a physical environment in which the web server and its clients run in a physical computer (figure 5). The web server is the Microsoft (MS) Internet Information Server (IIS) (http://www.microsoft.com/iis), which is functionally equivalent to the *Apache* web server. Like the *Apache*, the IIS operates in unsecured and secured modes. Downloading data files from the IIS can also be done interactively and non-interactively using the *Internet Explorer* web browser and the *wget* command, respectively. The *Internet Explorer* runs in the MS Windows XP OS, and the *wget* command runs in the *Cygwin* environment. *Cygwin* is an enabling technology that facilitates the use of popular UNIX and Linux applications on MS Windows environments. The virtual and physical network infrastructures can also be used within the same notebook computer as depicted in figures 6 and 7.

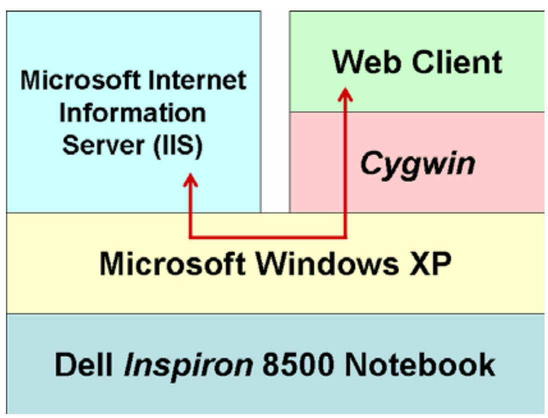


Figure 5. Physical Network Environment (PNE).

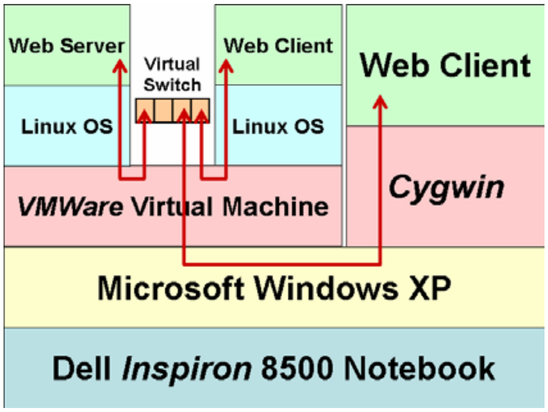


Figure 6. Server runs in VNE, client in PNE.

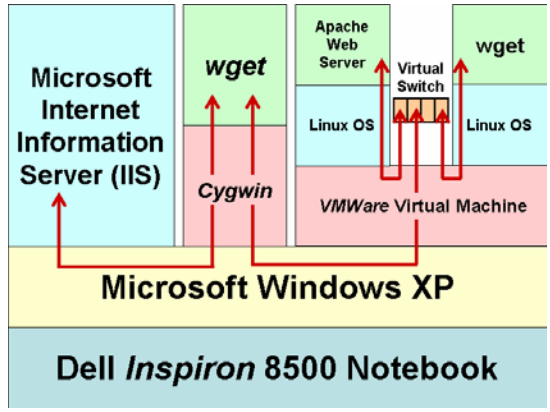


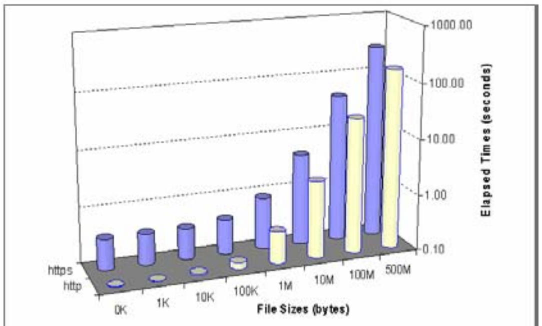
Figure 7. Server runs in PNE, client in VNE.

From the perspective of an end user, the performance of a web server is often measured in terms of elapsed times, which answers the question: How much time does downloading a file from a Web server take? Comparative measurements of the performance of a web server operating in secured mode and unsecured mode provide a quantitative performance cost associated with the deployment of a Web security product. Within the scope of this task, the security product is the transport layer security (TLS) that the hypertext transfer protocol (HTTP) uses. The use of HTTP over the TLS is commonly known as HTTPS. The use of HTTPS in the Internet requires a public-key infrastructure upon which basic IA services can be provided by a mutually trusted third party e.g., Verisign (http://www.verisign.com). The https enables electronic commerce over the Internet.

The two test bed environments used in this task issued their own digital certificates, which were required for running the two Web servers in secured mode. This was done because the test beds were isolated networked systems; they had no connections to the Internet. Therefore, obtaining real-time IA services from a third party was not possible. Appendix A shows the screenshots of the two self-signed digital certificates that were used by the *Apache* web server and the MS IIS Server.

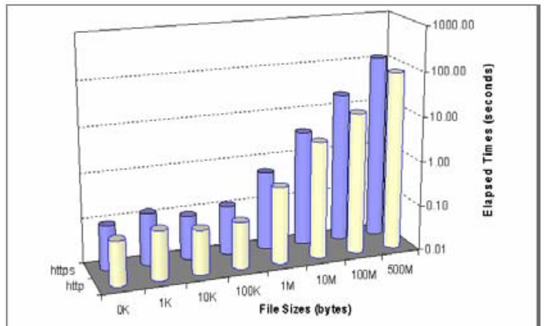
Comparative measurements performed during the performance period include four different combinations of virtual and physical environments running in the same notebook computer. The first experiment employed the virtual network environment (VNE) in which both the server and the client ran (figure 4). The second experiment engaged the server in VNE and the client in the physical network environment (PNE) (figure 6). The third experiment ran the server in PNE and the client in VNE (figure 7). The last experiment set up the client and the server to run in PNE (figure 5).

In each experiment a set of data files having various sizes was created and populated at the server to simulate various sizes of electronic archives. The client extracted each data file 100 times in secured and unsecured mode. Using the actual elapsed time of each session, the average elapsed time was calculated for each file and for each operational mode. Figure 8s through 11 numerically and graphically show the average elapsed times of the four different experiments.



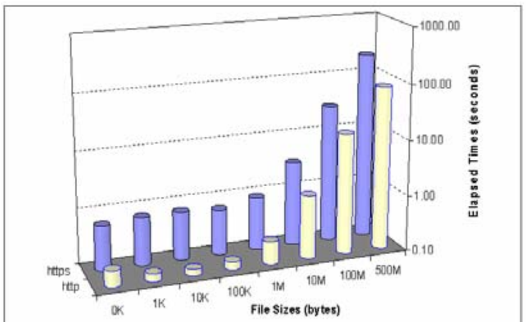
	0K	1K	10K	100K	1M	10M	100M	500M
http	0.10	0.10	0.11	0.13	0.38	2.44	26.70	166.55
https	0.36	0.36	0.36	0.42	0.87	4.41	43.73	290.88

Figure 8. Server and client in VNE.



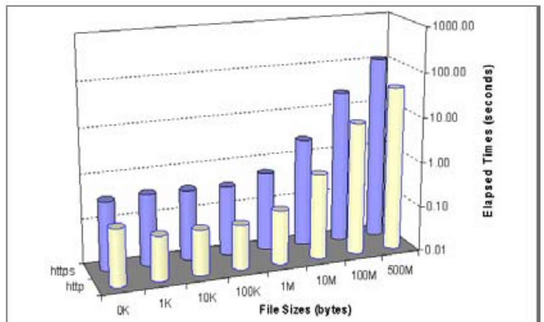
	0K	1K	10K	100K	1M	10M	100M	500M
http	0.10	0.12	0.10	0.11	0.50	3.93	13.75	91.24
https	0.10	0.14	0.09	0.12	0.56	3.66	21.09	123.89

Figure 9. Client in VNE, server in PNE.



	0K	1K	10K	100K	1M	10M	100M	500M
http	0.19	0.14	0.13	0.14	0.26	1.39	14.50	85.39
https	0.63	0.72	0.74	0.66	0.90	3.24	29.69	220.02

Figure 10. Client in PNE, server in VNE.



	0K	1K	10K	100K	1M	10M	100M	500M
http	0.18	0.10	0.10	0.10	0.16	0.78	8.62	43.66
https	0.35	0.38	0.37	0.36	0.56	2.57	24.22	120.73

Figure 11. Server and client PNE.

Using the computed averages, the performance costs in term of percentages were calculated, and the results are shown in table 2 and figure 12. The costs follow the same trend in that they decrease as the sizes of the transferred data files increase. This phenomenon could be explained in the following paragraphs.

Table 2. Performance costs.

Performance Costs	0K	1K	10K	100K	1M	10M	100M	500M
Server and Client in VNE	255%	258%	245%	218%	131%	81%	64%	75%
Client in VNE, Server in PNE	-1%	13%	-2%	11%	12%	-7%	53%	36%
Client in PNE, Server in VNE	223%	432%	473%	370%	249%	134%	105%	158%
Server and Client in PNE	90%	291%	266%	263%	255%	230%	181%	177%

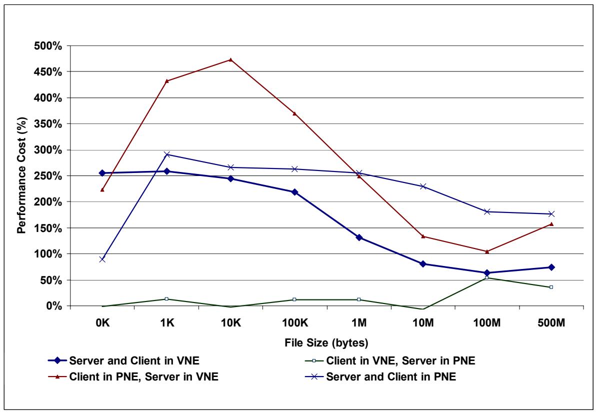


Figure 12. Performance Costs.

Each time a Web client downloads a file from a Web server, it needs T_c seconds to establish a connection to the Web server, T_t seconds to transfer the file, and T_d seconds to destroy the connection once it has completed the transfer. For a given network configuration and condition, T_t increases proportionally to the size of the data file, and T_c and T_d stay practically constant whether a communication session is in secured or unsecured mode. Therefore, the time T_p taken to transfer a file from a Web server is the sum of T_c, T_d, and T_t ; *i.e.*, $T_p = T_c + T_d + T_t$.

To transfer a file in secure mode, the Web client requires an additional T_a seconds to authenticate the server and to negotiate with the Web server for the use of an appropriate cryptographic algorithm and to exchange a cryptographic key and T_e seconds for the server to encrypt the data file and for the Web client to decrypt the encrypted file. Given the same network environment, T_a stays theoretically fixed, and T_e increases as the size of the data files increases. Thus, the required time, T_s, for transferring a data file from a secured Web server is the sum of T_p, T_a, and T_e; *i.e.*, $T_s = T_p + T_a + T_e$. The performance costs in term of elapsed time, T_{costs}, is the difference between T_s and T_p; *i.e.*, $T_{costs} = T_s - T_p = (T_p + T_a + T_e) - T_p = T_a + T_e$. The performance costs in term of percentages, $T_{percent}$, are calculated as follows: $T_{percent} = 100(T_s - T_p)/T_p$.

3.2.3 Conclusions

Experiments that were conducted completely in the VNE generated more credible performance data than any other experiments that were conducted in any other configuration as figure 12 indicates. This fact could be attributable to the efficacy of virtual machine technology, especially the VMW are software, that enabled the set up of a virtual infrastructure environment consisting of virtual network devices and virtual machines running actual operating systems and applications.

The use of virtual machines in this task also generates several side benefits that entice further investigation of the underlying technology to build future VNEs in which evaluations of untrusted software applications can be safely conducted and malicious attacks can be generated to evaluate the defensive mechanisms of the portal. Current virtual machine technologies can enable the building of an investigational network to conduct empirical experimentations of defensive IA technologies to evaluate their capability to secure and protect sensitive presidential ERA. Defensive IA products are software products that are deemed appropriate for the protection of the computing systems and networks that store, transmit, and process sensitive ERA. The ability of virtual machines to realistically represent a physical machine enables the building of a heterogeneous computing environment with much lower costs and convenience. Other benefits include: (i) the complete control of all types of network traffic generated in the test bed, (ii) the facilitation of system performance evaluation and measurement of the overhead associated with a deployed security product, and (iii) the complete independence from organizational administrative networks and their administrators. The current virtual network established in this phase of the research was a single network, and it can be extended to interconnect several sub-networks to reflect actual network environments, depending on the availability of computing resources.

3.3 Task 4. IA Product (Firewall) Assessment and Deployment

The scope of this task was to investigate potential IA technologies that can be used in the protection of the PERPOS portal, situated inside the GTRI research enclave environment. The portal is being built using commercial-off-the-shelf (COTS) security technology and government-validated IA products such as firewalls, intrusion detection systems, and antiviral software. The task was also to collaborate with GTRI researchers to acquire, install, and operate the security products and to develop a set of research performance metrics potentially applicable to the measurement of the efficacy of the deployed IA products in a test bed. Initial estimated level of effort: .1 FTE years.

3.3.1 Status

The level of effort of this subtask was underestimated; therefore, an additional .2 FTE, taken from the Subtask 5, and $2,400 training costs were allocated to this subtask. Son Nguyen of ARL-Atlanta joined the ARL team on January 13, 2004. Since then, he has been collaborating with the GTRI team and completed reviewing and evaluating 30 government-validated firewall products based on four criteria: technical merits, common criteria, novelty, and functionality. He also performed a literature search on defensive security technologies to determine optimal configuration and implementation of firewalls and intrusion detection systems and collaborated with GTRI researchers to develop a local security policy for the PERPOS portal. To acquire necessary knowledge for expeditiously implementing the firewall to protect the PERPOS portal, he attended a hands-on technical training course entitled “Deployment Internet and Intranet Firewalls: Hands-On.” The findings and recommendations of this task are being acted on by the GTRI team to acquire and deploy an appropriate and effective firewall to protect the PERPOS portal.

3.3.2 Results and Discussions

A firewall is used to regulate traffic by deciding which types of traffic are allowed to enter and leave a network. A firewall can prevent most of the attacks from unwanted penetration if designed, configured, and maintained properly. Along with other information assurance tools, a firewall plays a major role in protecting the network from malicious activities such as denial of service, scanning, and sniffing both from inside and outside the network, and enforces network security policies.

Basically, there are three types of firewalls: packet filter, stateful inspection, and application proxy, ranging from early and simple to recent and complicated technologies. Packet filter is the most basis form of firewall with a fundamental task to filter the traffic based on the information contained in a packet header, the IP or TCP/IP layer, with IP address and/or port number. Because the firewall does not have a function to keep track of a TCP session, spoofed packets can go along, unable to be detected, and, therefore, can easily seep through the firewall. In order to stop spoofed packets, packet filter firewall with stateful inspection functionality has a capability to keep track of the network session by matching the packet to the corresponding entry in the connection table. However, this technology can only check and control the traffic based on the packet header. The even more secure firewall, called application proxy, has higher level of packet screening which can analyze packets all the way up to the application layer. In addition, the firewall plays an intermediary role to separate user's machine (source) with an intended host (destination), preventing direct communications between users and host in order to avoid any attacks on the internal hosts 0.

In addition to controlling the traffic, many firewalls now have additional integrated features, such as virtual private network (VPN), to provide end-to-end communications security using the strongest levels of encryption to protect the privacy of data transmitted over the unprotected Internet. This feature helps eliminate the cost for leased lines and provides confidentiality, integrity, and authentication for the connections. In general, there are two types of connections using VPN: between two sites (gateways) and between site and client (mobile user).

In a review of thirty (30) National Information Assurance Partnership (NIAP)-validated firewall products in order to select the best product for the PERPOS network, the following criteria were used:

- NIAP-validated product, compliant with NIAP Common Criteria requirements, EAL4
- In conformance with technical requirements as specified in the security policy
- Latest technologies
- Widely supported (strong customer base)

First, the product must meet the NIAP Common Criteria requirements. That means in this case the firewall must go through the NIAP Common Criteria evaluation/validation process to meet all the requirements of the International Standards Common Criteria. For the Evaluation Assurance Level (EAL), the highest currently most products can meet is level 4, Medium Level, where EAL1 is the lowest, and EAL7 is the highest (*7*).

The next selection criterion is to satisfy the technical requirements. In this case, the product must meet or exceed the requirements specified in the security policy document. For example, the type of services and traffic that can go through the firewall should or should not be controlled. Protection of the firewall must provide a certain security level and prevent attacks or violations from both sides of the wall. Network address translation, port address translation, VPN, encryption, and number of customers are the few basic requirements to be satisfied. How much traffic bandwidth is the minimum requirement for the firewall to support? Is the site expected to grow? Are remote access services required?

The third selection criterion is the latest technologies. With a restriction of using the NIAP-validated product, sometimes it is difficult to obtain the latest release version of the system available on the market. It requires time for the product to go through the test/validation process to be ready. Hence, the selection should be as most recent as possible. Finally, the last criterion (widely supported by the vendor) is not only beneficial to the implementation of the product, but also helpful for the interoperation with other types of products as well.

Two products having the highest scores are Symantec's products and Check Point's product as shown in table 3.

Table 3. Firewall evaluation results.

Product	Meet Technical requirements	Latest Technology	Support	NIAP	Total Score
Borderware, Borderware Technologies	7	6	7	6	26
Check Point, Check Point SW Tech.	9	8	9	8	34
Check Point, Nokia	9	10	9	8	36
3Com Embedded, Secure Computing	7	8	8	4	27
Cisco Secure PIX, V5.2, Cisco	7	7	9	7	30
Cisco Secure PIX, V6.2, Cisco	9	8	9	8	34
Conceal Private, Signal 9 Solutions	6	6	5	2	19
CS Bastion II, ClearSwift	7	8	6	7	28
CyberGuard, CyberGuard Corp	9	9	8	8	34
DiamondTEK, Cryptek Secure Comm.	7	7	6	4	24
ETM, SecureLogix Corp	7	8	6	5	26
Enterprise Tele Mgmt, SecureLogix	7	7	6	5	25
Gaunlet, Secure Computing	8	8	7	7	30
Internet Security, Microsoft	8	8	8	5	29
Lucent VPN, Lucent Technologies	8	8	7	5	28
Netscreen Model 5XP, Netscreen Tech	7	8	7	7	29
Netscreen Model 5200, Netscreen	9	8	8	8	33
Netscreen 204, Netscreen	7	8	7	7	29
Netscreen 4.0.0, Netscreen	7	8	7	5	27
Nortel Alteon Switched, Nortel	7	8	7	7	29
Safegate, Fujitsu Limited	7	7	6	6	26
SECUREWORKS, Oullim Info. Tech	7	7	6	6	26
Sidewinder, V5.2.1, Secure Comp	8	7	8	5	27
Sidewinder, V6, Secure Comp	8	8	8	8	32
Stonesoft StoneGate, Stonesoft	9	9	8	8	34
Symantec, v7.0.4, Symantec Corp.	9	8	9	8	34
Symantec, v7.0, Symantec Corp.	8	8	9	8	33
Symantec, v2.0, Symantec Corp.	9	10	9	8	36
TeleWall System, SecureLogix	7	7	6	4	24
Watchguard LiveSecurity, Watchguard	6	7	6	4	23

3.3.3 Recommended Products

3.3.3.1 Symantec Enterprise Firewall with VPN 7.0

The Symantec Firewall provides two basic functionalities: controlling the information traveling through it and protecting the information sent from site to site and from a remote client to site using VPN capabilities. Here are some basic features of the product (*8*):

- Application-Layer Proxy: The firewall provides full application level inspection in addition to circuit-layer protection and packet filtering as in conventional firewalls. This inspection allows a complete check of all levels of the protocol stack to detect and prevent attacks inserted in every level.

- Built-In support for popular protocols: Covers most popular protocols.
- High Speed Performance: Firewall throughput exceeds common network connection such as ATM OC-3 (155 Mbps), and slower networks such as Fast Ethernet, etc.
- Integrated VPN Support: Provides secure, high-speed connection between site to site and site to client using IPSec security protocol, with AES, DES, Triple DES encryption to protect data, and IKE key management for user authentication and key exchange.
- Operating System Hardening: Built-in detection mechanism to protect itself from intrusion.
- Port Blocking: Automatically blocks all unauthorized TCP and UDP.
- Anti-Spamming and Anti-Spoofing: Protect email servers from spamming and prevent unauthorized access to internal systems.
- Centralized, Remote Management: Equipped with Symantec Raptor™ Management Console, a graphical user interface, to help create and enforce security policy, receive automatic alerts for specified log events, and generate detailed reports.
- Platform Requirements:
- Solaris: Single processor, 400 MHz, Solaris 7/8 UltraSparc I/II, 256 MB RAM, 8 GB disk space, CD-ROM drive, at least 2 NICs.
- Windows NT/2000: Intel Pentium III, 400 MHz, 256 MB RAM, 8 GB disk space, CD-ROM drive, and at least 2 NICs.
- Price starts from $2,100 and up depending on the number of users and platform used.

3.3.3.2 Symantec Enterprise Firewall with VPN 8.0 (recent release)

This Symantec version was recently released with the addition of many advanced features compared with its previous version. These features include:

- Use of web-based as a graphical user interface for Security Gateway Management
- Advanced centralized management tool: provides centralized configuration, event logging, alerting and reporting.
- State-sharing Integrated High Availability/Load Balancing: In the case of failure with multigateway, firewall and VPN sessions will failover automatically to another gateway.
- Platform requirements:

- Solaris: Sun Solaris 8 (32 & 64-bit), Solaris 9 (64-bit)
- Windows 2000: Microsoft Windows Server 2000, Advanced Server 2000, Server 2003.
- Note: This version 8.0 is NIAP-validated with EAL level 4, as confirmed by a Symantec Representative.

3.3.3.3 Check Point Firewall-1/VPN-1, Nokia IP350

The Check Point Firewall-1/VPN-1, Nokia IP350, full-featured designed for small and medium enterprises, operates in two modes: (1) supervising all traffic passing between networks connected to the firewall by inspecting packets, blocking all unwanted access attempts, and (2) protecting communication channel over the Internet (public network) between two Check Point Firewalls or a Check Point Firewall and a SecureClient 0.

- Stateful Inspection Technology: The firewall enforces its security policy and desktop security policy by taking action one of the following operations: either accepting the IP packet flow between the source and destination, or rejecting with notifying the source, or dropping without notifying the source. It also inspects traffic from data link layer to application layer.
- Internet Protocols: Cover most popular Internet Protocols.
- High Speed Performance: The firewall throughput for large packets is up to 350 Mbps, with VPN throughput for large packets up to 80 Mbps, 3DES, AES.
- Integrated VPN Support: Enables secure connectivity between sites, remote offices and users.
- Management and remote supervision: Equipped with management tools such as Nokia Horizon Manager, Network Voyager, etc., to simplify installation, configuration, management, and maintenance.
- Anti-Spoofing: Administrator can create a filter with particular sets of network addresses either to allow, reject, or drop a packet which each conforms to the allowed set of networks for particular interfaces and for the direction of movement.
- Data Filtering: Capable of having FTP, HTTP and SMTP based connections diverted to an interface for packet content analysis, as a precondition for accepting.
- IP security platform for the small enterprise: combined with the Nokia IPSO™ secure operating system which is the industry-proven hardened Nokia operating system with web-based element management interface and Command Line Interface.
- Audit: Capable of generating audit records, logs, and alerts corresponding to audit events.

3.3.4 Conclusions

- Performance vs. security level: Symantec products provide very high protection with all-level inspection and prevent outsiders from reaching the protected hosts, when compared for security with Check Point Product. Since it takes extra processing time to provide full application inspection, it Symantec products could suffer on performance comparisons, with less than half the throughput compared with others.
- Convenience vs. price: Unlike Symantec products, the Nokia product offers two choices to customers: either software part or both; a complete system, ready to plug and play. In addition, the system has been hardened, thus eliminating any security holes.
- Problem with NIAP-validated products: It takes time to go through NIAP-validation/certification process. Therefore, many recent releases with the latest technologies and less vulnerabilities do not meet such a requirement.

4. Canceled Tasks

ARL canceled Tasks 2 and 5 because it needed to reassign and redeploy technical personnel previously allocated for completing the planned tasks. The cancellation was unavoidable as ARL is actively supporting the OIF, which is currently the number one priority for the security of America. The remaining funds are being used for completing Task 4 and for the next phase activities.

4.1 Task 2. Commercial Product Assessment

This task was to investigate and assess the effectiveness of COTS Web-based IA technologies to reasonably secure a portal test bed operating in unsecured public network to support authentication, confidentiality, integrity, and non-repudiation in distributed, heterogeneous ERA. Level of effort: .1 FTE years.

4.2 Task 5. Implementation and Deployment Issues

Investigate implementation and deployment issues of IA products and research optimal methods and techniques for the integration, protection, and management of cryptographic products for contribution for preservation, management and access to Presidential electronic records collections and other files of the Federal Government. This task includes three subtasks: (1) assessing the feasibility of potentially appropriate cryptographic products to sufficiently secure and protect the confidentiality of electronic records traveling across an unsecured public network, (2) identifying potentially appropriate communication layer(s) where the encryption could be performed and assess the complexity associated with each alternative, and (3) identifying and assessing applicable technical, financial, and operational issues associated with an evaluation and selection of a particular cryptographic algorithm and protocol potentially appropriate to protect electronic records archive subject to heterogeneous sensitivity levels. Estimated level of effort: .7 FTE years.

5. Professional Activities

5.1 Publications

The following efforts were undertaken to assess the State-of-the-Art (SOTA) and State-of-the-Practice (SOP) in IA activities as they pertain to technologies used in creating, accessing, and maintaining distributed ERAs. Collaborations and dissemination of research activities are intended to leverage ongoing activities, methodologies, and technologies (to include hardware/software) that can be used to mitigate and solve issues and problems associated with developing an operating environment of distributed ERAs.

Four technical papers by the PI have been accepted for presentation at the conferences and publication in their associated proceedings. Therefore, with the support and encouragement of ARL, the PI attended the conferences to present research results from performing the NARA-sponsored work on distributed ERA. All presented papers relate to technical aspects of IA and distributed ERA processing. By attending these conferences, the PI had the opportunities to share his research findings and simultaneously to learn about the latest advances in security and computing techniques potentially applicable to the safeguarding of distributed ERA.

Below is a list of the papers generated during the performance period of this work, and the names of the conferences at which the papers were presented.

Presented Paper Title	Author	Conference Name, Location, and Dates
A Virtual Test Bed for Distributed Processing of Archives	Binh Nguyen	The 4th World Scientific and Engineering Academy and Society International Conference on Information Science, Communications and Applications in Miami, FL, April 21-23, 2004
Security Issues and Requirements for a Web Portal of Sensitive Archival Records	Binh Nguyen	The 3rd Security Conference, Las Vegas, NV, April 14-15, 2004
A Security Architecture for a Web Portal of Sensitive Archival Records	Binh Nguyen	The 2004 International Conference on Security and Management, Las Vegas, NV, June 21-25, 2004
Mobile Agents for Distributed Processing of Electronic Records Archives	Binh Nguyen	The 2004 International Conference on Information and Knowledge Engineering, Las Vegas, NV, June 21-25, 2004

5.2 Travel

During the performance period, Mr. Glenn Racine, the program manager took 2 trips to Atlanta, GA to discuss this project with GTRI researchers.

5.3 Training

Training Course	Trainee	Trainer	Training Period	Course Location
Deployment Internet and Intranet Firewalls: Hands-On	Son Nguyen	Learning Tree International	1-4 Jun 04	Atlanta, GA

6. Conclusions and Recommendations

Initial results generated during the performance period provided encouraging evidence that (i) the concept of defense in depth can also be implemented successfully at GTRI to secure and protect the portal of sensitive archives, (ii) the evaluation method and its associated software tools can be employed to measure the performance overhead in terms of time incurred at the actual physical Web portal, and (iii) the use of government-validated defensive security products at the portal will provide NARA with reasonable assurance that sensitive ERA can be secured and protected.

For the coming efforts, ARL recommends the following tasks be conducted in FY05:

Conduct empirical experiments to evaluate the performance overhead induced by the deployment of defensive IA products at the actual PERPOS portal operating in unsecured and secured mode. The overhead will be measured in terms of elapsed times *and* computing times taken at the client computer. The experiments will be conducted at the Adelphi facility of ARL using a simulated Web server if the physical PERPOS portal is not ready for experimentation. The results of these experiments will assist in the acquisition of appropriate technological and security products capable of meeting the future operational requirements of sensitive ERA portals.

Conducting live experiments requires substantial funding for building a physical computing network infrastructure. However, these costs can be substantially reduced or eliminated by leveraging the existing resources at ARL and at GTRI. The experimentation will continue to focus on scientifically assessing, analyzing, and mitigating potential threats to irreplaceable ERA.

Continue assessing other types of government-validated IA products suitable for the protection and the empirical experimentation of the actual PERPOS web server. Products that need to be evaluated will include intrusion detection systems, antiviral software, and security management tools. ARL personnel in Atlanta will collaborate with GTRI researchers in investigations directed to defensive IA products and develop a set of research performance metrics potentially applicable to measuring the efficacy of the IA products deployed to protect and secure the physical PERPOS portal.

7. References

1. Thibodeau, K. Building the Archives of the Future, D-Lib Magazine. Vol. 7, No. 2, February 2001. URL: http://www.dlib.org/dlib/february01/thibodeau/02thibodeau.html (accessed 13 Jan 04).

2. National Security Agency, *Information Assurance Technical Framework*, Release 3.1, September 2002, National Security Agency, Fort Meade, Maryland, 20755-6730, URL: https://www.iatf.net/ (accessed 15 January 2004).

3. National Information Assurance Partnership, Common Criteria, *Validated Products*, URL: http://niap.nist.gov (accessed 15 January 2004).

4. Ford, W; Baum, M. *Secure Electronic Commerce*, 2nd Ed, Prentice Hall PTR, Upper Saddle River, NJ, 2001.

5. Maconachy, V.; Schou, C.; Welch, D.; Ragsdale, D. J. A Model for Information Assurance: An Integrated Approach, *Proceedings of the 2nd Annual IEEE Systems, Man, and Cybernetics Information Assurance Workshop,* West Point, NY, June 5-6, 2001, 306–310.

6. Wack, J.; Cutler, K.; Pole, J. *Guidelines on Firewalls and Firewall Policy*, NIST, Special Publication 800-41, January 2002, pp. 3–15.

7. Common Criteria for Information Technology Security Evaluation, Common Criteria, Part 3: Security Assurance Requirements, August 1999, Version 2.1, CCIMB-99-033, pp. 53–67.

8. Security Target for Symantec Enterprise Firewall for Windows NT, Version 7.0, May 2002, Symantec Corp.

9. Common Criteria EAL4 Evaluation, Check Point Software Technologies Inc., VPN-1/Firewall-1 Next Generation (Feature Pack 2), July 2003.

INTENTIONALLY LEFT BLANK

Appendix A. Screenshots

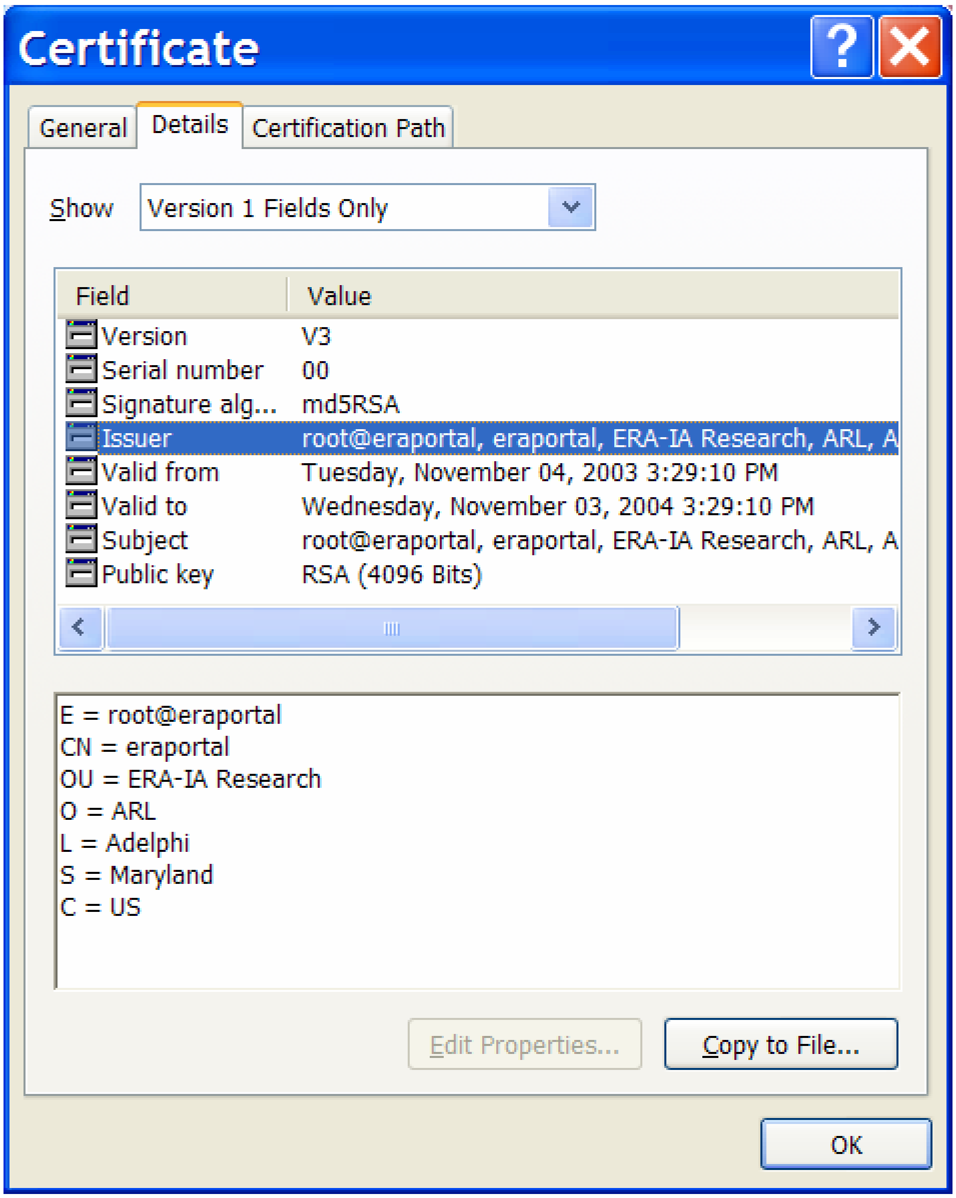


Figure A-1. Self-Signed Certificate Screenshot 1.

This self-signed certificate enabled the Apache Web server to operate in secured mode in support of the measurement of its performance in secured and unsecured mode.

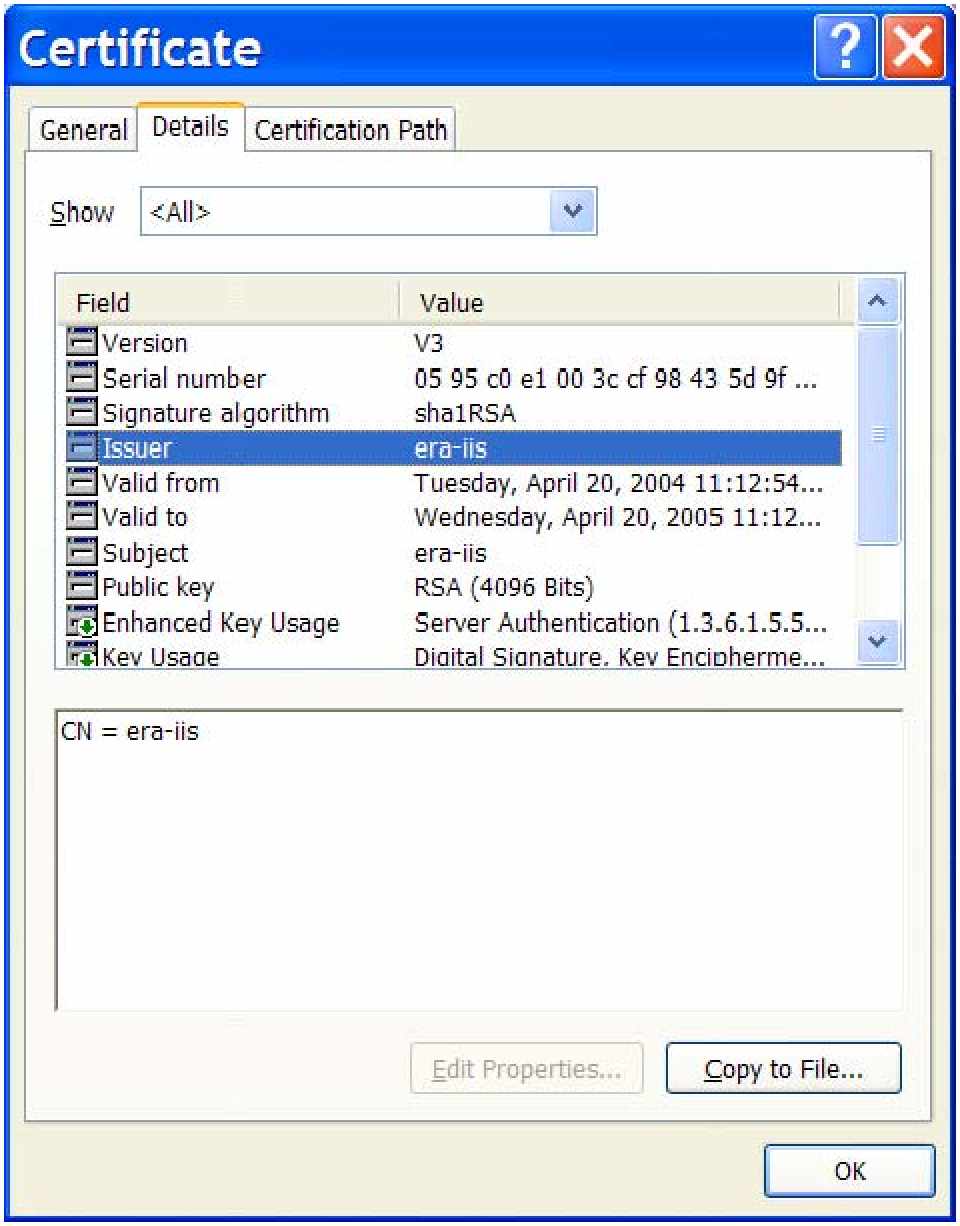


Figure A-2. Self-Signed Certificate Screenshot 2.

This self-signed certificate enabled the Microsoft Internet Information Server to operate in secured mode in support of the measurement of its performance in secured and unsecured mode.

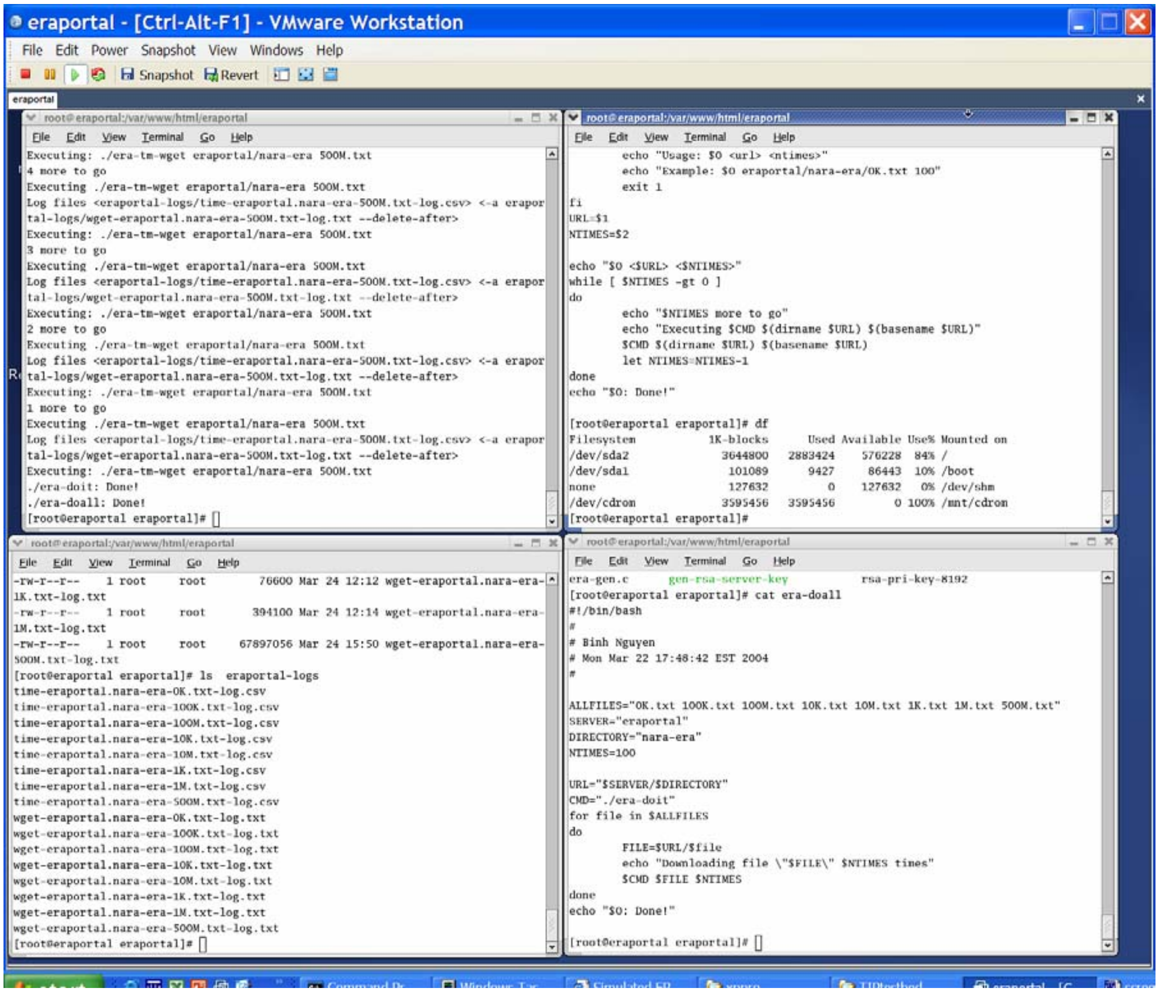


Figure A-3. MS Windows-based Virtual Machine Running Linux OS.

INTENTIONALLY LEFT BLANK

Distribution List

ADMNSTR
DEFNS TECHL INFO CTR
ATTN DTIC-OCP (ELECTRONIC COPY)
8725 JOHN J KINGMAN RD STE 0944
FT BELVOIR VA 22060-6218

NATL ARCHIVES & RECORDS ADMIN
ELECT RECORDS ARCHIEVS PROG MGMT OFC
ATTN R CHADDUCK (5 COPIES)
8601 ADELPHI RD
COLLEGE PARK MD 20740-6001

GEORGIA TECH RESEARCH INSTITUTE
ATTN W UNDERWOOD (2 COPIES)
ATLANTA GA 30332

US ARMY RSRCH LAB
ATTN AMSRD-ARL-CI-CT S NGUYEN
(5 COPIES)
115 O'KEEFE BLDG. GITA
ATLANTA GA 30332-0800

US ARMY RSRCH LAB
ATTN AMSRD-ARL-CI J D GANTT
(2 COPIES)
ATTN AMSRD-ARL-CI-C J GOWENS
ATTN AMSRD-ARL-CI-CN B NGUYEN
(5 COPIES)
ATTN AMSRD-ARL-CI-CN G RACINE
(5 COPIES)
ATTN AMSRD-ARL-CI-OK-T TECHL PUB
(2 COPIES)
ATTN AMSRD-ARL-CI-OK-TL TECHL LIB
(2 COPIES)
ATTN AMSRD-ARL-D J M MILLER
ATTN IMNE-AD-IM-DR MAIL & RECORDS
MGMT
ADELPHI MD 20783-1197

INTENTIONALLY LEFT BLANK.